U.S. GOVERNMENT-WIDE INCIDENT RESPONSE CAPABILITY

Marianne Swanson
Computer Security Division
National Institute of Standards and Technology

Abstract

This paper describes the many functions that a federal incident response capability (IRC) would perform and explores the issues that should be addressed prior to the establishment of an IRC. The need for an incident response capability that crosses agency boundaries has never been greater. Almost all federal agencies are now connected to the Internet and exchange information regularly. The number of Internet related incidents that have occurred in the past year, along with the increase and complexity of viruses, requires agencies to take seriously their incident handling capability. The Office of Management and Budget has reinforced this need by requiring in the revision to OMB Circular A-130, Appendix III, that agencies be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. A government-wide incident response capability (IRC) would assist civil agencies in meeting this requirement.

Introduction

The need for an incident response capability that crosses agency boundaries has never been greater. Almost all federal agencies are now connected to the Internet and exchange information regularly. The number of Internet related incidents [*figure 1.*] that have occurred in the past year, along with the increase and complexity of viruses, requires agencies to take seriously their incident handling capability. The Office of Management and Budget has reinforced this need by requiring in the revision to OMB Circular A-130, Appendix III, that agencies be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. A government-wide incident response capability (IRC) would assist civil agencies in meeting this requirement. This paper describes the functions an IRC would perform and explores the issues that need to be addressed prior to the establishment of an IRC.

Background

The concept of a government-wide computer incident response capability has been researched and reported on since the Forum of Incident Response and Security Teams (FIRST)[1] was created in

[1] FIRST is an international group of incident response teams whose goal is to foster communication to prevent and to rapidly handle computer security related incidents.

1989. The original concept of how FIRST would coordinate the many incident response teams within the FIRST organization, depict vendor teams, service provider teams, foreign government teams, U.S. military teams, several large U.S. federal teams, and one central U.S. federal team that would coordinate incident handling and information collection and dissemination for all other federal agencies. In the early 1990s, most agencies were not connected to the Internet and, except for cleaning up viruses, very few offered any formal incident handling support. The timing for the development of a government-wide IRC was too early.

CERT(sm) Coordination Center Statistics

Year	Incidents Reported(1)	Mail Messages Received	Requests Received(2)	Information Hotline Calls Received(3)
1988	6	539		
1989	132	2867		
1990	252	4448		
1991	406	9629		
1992	773	14463	275	1995
1993	1334	21267	1270	2282
1994	2341	29580	1527	3664
1995	2412	32084	1683	3428

Footnotes

(1) An incident may involve one site or hundreds or thousands of sites. Also, some incidents consist of ongoing activity for long periods of time (e.g., for more than a year).
(2) Information requests have been tabulated beginning July 1992. This number does not include requests to be added to mailing lists.
(3) Incoming hotline calls have been tabulated since January 1992. This number does not reflect total telephone activity related to incidents because outgoing calls made by CERT staff are not included.

Figure 1.

The IRC concept was again explored in 1993 by the National Security Telecommunications and Information Systems Security Committee (NSTISSC). This proposed plan for a national level IRC was limited in scope in that it would handle incidents affecting national security systems within military sites and civil sites. The report was presented to the NSTISSC member agencies in January 1993. The agencies agreed with the concept but could not support the resource commitment.

Recently, several other organizations have proposed an IRC concept. The General Services Administration, the National Communications System, and the National Institute of Standards and Technology have all prepared proposals to various funding bodies to obtain the much needed capital to seed such an enormous task. The outcome of these proposals -- whether they were approved, partially approved or turned down -- has yet to be determined. Clearly, there are many organizations that believe a national coordination of incident handling and a sharing of vulnerability related information is needed and needed soon

Scope

The IRC proposed by NIST is to provide a cost reimbursable incident handling service for those agencies not having sufficient resources to support their own capability. The IRC would facilitate the sharing of vulnerability information that would assist agencies in protecting their systems against known threats. The objective of the IRC would be to develop a self-sustaining incident response capability that meets the need of the federal agencies. Activities would range from providing agencies with direct technical support to handle computer security incidents, to providing backup support to agency response teams dealing with large and complex incidents, to providing agency response teams with information on threats, vulnerabilities, and countermeasures that allow agency teams to effectively deal with incidents on their own. Proposed activities include:

- Responding effectively and in a timely manner to security incidents: Coordinate the analysis of the problem, determine the magnitude of the threat, provide technical assistance in identifying and closing vulnerabilities, notify sites affected, and issue advisories to the agencies warning of the problem and describing countermeasures.

- Expanding the limited coverage of existing agency computer response teams by providing a broader range of incident types and technologies.

- Providing agencies with guidelines on implementing "fixes" and other security controls.

- Maintaining a 24 hour, 7 days a week response service for emergencies and a "Help Desk" function for normal business hours.

- Facilitating the interaction with law enforcement agencies in the reporting of security incidents involving violations of the law.

- Assisting federal law enforcement in evidence gathering, where appropriate.

- Coordinating with other organizations including FIRST.

- Developing, distributing, and maintaining publicly available security tools, incident handling tools and data gathering and reporting tools.

- Coordinating with vendors and Internet service providers to provide critical security patches and "work-arounds."

- Performing vulnerability analysis to identify a vulnerability's root-cause in order to identify other potential problems before they occur.

- Keeping the federal community aware of the current threat, i.e., education in current technology and associated threats; training of security and network administrators on security practices; and awareness through world wide web sites, ftp services and guidance documents.

The IRC would act as the central point of coordination and would establish channels to address incidents and vulnerabilities affecting agencies. A method for collecting, analyzing, and disseminating sanitized vulnerability, threat, and incident data would be developed. Activities in this area would include:

- Developing an acceptable use policy that defines the ways in which vulnerability data would be stored, protected, disseminated and used.

- On-going development of product vulnerability reports that describe product vulnerabilities along with known corrections, work-arounds, or countermeasures.

- On-going development of reports on intruder tools and techniques that describe methods of attack, potential impact, and countermeasures.

- Analyzing vulnerabilities to identify root-causes of problems in product development practices that produced the flaws and to support the development of tools that can test for other instances of similar flaws.

- Incident follow-up studies to identify the cause of the incident, operational impact on the affected organizations, and cost of resolving the incident, of recovering lost or damaged data, of restoring operation and of lost productivity.

Benefits

The primary benefits of this program would be:

- The immediate availability of the type of technical expertise and assistance that agencies need now to handle computer security incidents. The IRC will augment existing agency teams and provide assistance for agencies therefore, reducing the need to develop “full-function” incident response capability.

- The impact of security incidents will be contained and minimized by reducing the number of vulnerabilities among federal systems and by providing an early warning system that allows agencies to protect themselves from new threats.

- A centralized organization will review the nature of attacks to federal systems and will provide a common set of recommendations, tools and training to reduce the overall risk to federal systems.

Issues

To undertake a project with such far reaching goals, many questions must be answered. This paper does not attempt to answer them, rather the issues to each question are explored.

How to fund the capability? The biggest hurdle experienced so far is how to fund the IRC capability. Start up capital is required in order to be in a position to offer services immediately. Agencies need to get a return on their money and obtain the needed support; they are not in a position to wait six months or a year until the capability is staffed, trained and has the equipment to respond. If start up capital is secured, how to become self-sustaining is the next hurdle. All services would require an associated fee with possible plan options that agencies could buy into. For example, an agency may want to pay $25k for five days of incident handling support or $75k for a year of incident handling support for one firewall and all the systems connected to it. The fee structure should take into account all the functions the IRC would offer and price them competitively, yet reasonably enough for federal agencies to use them.

Who is responsible for the IRC? What government agency or Department is to be responsible for the federal IRC? GSA is in a position to contract out services; the IRC could be a service similar to the contingency planning hot-site agreements that currently exist through GSA’s Federal Systems Integration and Management Center (FEDSIM). NIST could be considered a viable option for administering the contract and maintaining overall responsibility for its operation.

Who would operate the IRC? An existing team, like the Department of Energy's CIAC or like the CERT-CC, funded by DARPA, could take on the additional responsibility and workload and be ready to offer assistance immediately. By placing the IRC in an existing federal team, there would be no lag of six months or more until a new team is operational. The unique federal requirements would already be known. An argument can easily be made that a private incident handling team already in existence could be operational just as quickly and provide the same assistance as an existing federal team. The concept of placing the IRC within a federal agency and building it from the ground up should also be considered. By starting from scratch, the IRC can be built to exact specifications without the baggage brought in by an existing team.

What type of information should be handled? The NSTISSC report mentioned earlier described a need for a capability that would handle United States national security information. If a federal agency has an incident involving national security information, who does the agency go to for incident support? The DoD ASSIST team handles computer security incidents for military sites; does that include all classified incidents as well? Clearly, the IRC would need to work closely with the DoD teams to ensure that all national systems, including national security related systems, are supported if an incident occurs.

Conclusion

By having a centralized organization reviewing the nature of attacks, providing support, and sharing information, the security posture of federal systems are improved. The Administration recognized the need for incident handling and the sharing of incident and vulnerability data by establishing the requirement in the revision to OMB Circular A-130. With the requirement now in place, the time has finally come for a government-wide capability.

References

Culver, Grace. General Services Administration, *Draft Proposal: Federal Information Systems Security Incident Response Capability.* February 24, 1996.

CERT-Coordination Center, Software Engineering Institute. *Incident Statistics*. January, 1996.

Forum of Incident Response and Security Teams. *Operational Framework.* August, 1993.

National Institute of Standards and Technology. *Information Technology Fund Innovation Fund Pilot Program Proposal.* March 1, 1996.

National Security Telecommunications and Information Systems Security. *National Security Information Systems Incident Program (NSISIP*). January 1993.